PURPOSE

To provide the Michigan Department of Health and Human Services MDHHS (MDHHS) with effective monitoring, reporting, investigation, response, remediation, and, if necessary, timely breach notification to affected individuals, related to an information security incident as defined by this policy.

REVISION HISTORY

Issued: 6/01/2021.
Next Review: 6/01/2022.

DEFINITIONS

Breach

The unauthorized acquisition, access, use, or disclosure of confidential information, that compromises the security or privacy of the information.

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the SOM. Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency's business.

Electronic Protected Health Information (EPHI)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

Impermissible Use or Disclosure

The acquisition, access, use, or disclosure of confidential information in a manner not permitted under applicable confidentiality laws that may or may not compromise its security or privacy.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Includes privacy incidents involving the actual or potential unauthorized disclosure of personally identifiable information.

Information Spillage

Instances where confidential Information (such as Federal Tax Information) is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity.

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual’s identity (such as, name, Social Security Number, date and place of birth, mother’s maiden name, biometric records) including any other personal information linked or linkable to an individual.

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS must manage incidents negatively impacting the security and privacy of information, systems and related assets. This includes suspected or actual violations and breaches of privacy, that involve unauthorized or impermissible uses, or disclosures of specific types of confidential information, which must be identified, reported, documented, responded to, mitigated to the extent practicable, and evaluated for the implementation of breach notification procedures when required by law.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the incident response [IR] family of NIST controls managed by MDHHS in accordance with DTMB 1340.00.090.01, Incident Response Standard. MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)

- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

- Social Security Administration (SSA) Technical System Security Requirements (TSSR)

- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

Incident Response Plan Training [IR-2]

MDHHS must provide workforce members with incident response training consistent with assigned roles and responsibilities. Training should occur prior to authorizing access to the agency information system or performing assigned duties, when required by agency information system changes, and annually thereafter.

Incident Response Plan Testing [IR-3]

MDHHS must test the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results.

Incident Response Plan Testing – Coordination with Related Plans [IR-3 (2)]

MDHHS must coordinate incident response testing across organizational programs with responsibility for related plans. Such plans related to incident response testing include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

Incident Handling [IR-4]

MDHHS must:

- Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

- Coordinate incident handling activities with contingency planning activities.

- Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Incident Monitoring [IR-5]

MDHHS must track and document security incidents on an ongoing basis. Maintaining records about each information system incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Incident Reporting [IR-6]

MDHHS workforce members must immediately report all suspected or actual privacy and security breaches, incidents and violations, as required by MDHHS Administrative Policy APL 68E-130, Breach, Security Incident or Impermissible Use or Disclosure.

Incident Response Assistance [IR-7]

MDHHS Compliance and Data Governance Bureau must provide incident response support to employees and contractors who, as users of department-managed information systems, may have specific concerns or system-specific questions regarding the handling and reporting of security incidents.

Incident Response Plan [IR-8]

MDHHS must:

- Develop an incident response plan that:
    - Provides the organization with a roadmap for implementing its incident response capability.
    - Describes the structure and organization of the incident response capability.
    - Provides a high-level approach for how the incident response capability fits into the overall organization.
    - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.
    - Defines reportable incidents.
    - Provides metrics for measuring the incident response capability within the organization.

  - Defines the resources and management support needed to effectively maintain and manage an incident response capability.

  - Describes the roles, responsibilities, communication and incident response strategies.

  - Is reviewed and approved by designated incident response personnel.

- Distribute copies of the incident response plan to designated incident response personnel.

- Review the incident response plan at least annually, or as an after-action review.

- Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Information Spillage Response [IR-9]

When required based on data classification, MDHHS must respond to information spills by:

- Identifying the specific information involved in the information system contamination.

- Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill.

- Isolating the contaminated information system or system component.

- Eradicating the information from the contaminated information system or component.

- Identifying other information systems or system components that may have been subsequently contaminated.

ROLES AND RESPONSIBILITIES

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

Workforce members must report security incidents as soon as possible, in accordance with MDHHS policies, standards and procedures

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations

NIST 800-53 rev.4:

IR-1 Incident Response Policies and Procedures
IR-2 Incident Response Training
IR-3 Incident Response Plan Testing

IR-3 (2) Incident Response Plan Testing – Coordination with Related Plans

IR-4 Incident Handling

IR-4(1) Incident Handling Incident Handling - Automated Incident Handling Processes

IR-5 Incident Monitoring
IR-6 Incident Reporting
IR-6(1) Automated Reporting
IR-7 Incident Response Assistance
IR-8 Incident Response Plan
IR-9 Information Spillage Response

45 CFR §164.308(a)(1)

164.308(a)(1)(ii) D Information System Activity Review (R)

45 CFR §164.308(a)(6)

164.308(a)(6)(i) Security Incident Procedures (R)
164.308(a)(6)(ii) Incident Response and Reporting (R)

State Standards/Regulations

MDHHS Policy Manuals

APL 68E-130 Breach, Security Incident or Impermissible Use or Disclosure

DTMB Administrative Guide

DTMB IT Technical Policies, Standards and Procedures

1340.00.090.01 Incident Response Standard

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.